⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭62－166489

⑤Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　昭和62年(1987)7月22日
G 06 K 17/00		T－6711－5B	
G 06 F 15/30	350	A－8219－5B	
G 09 C 1/00		7368－5B	審査請求　未請求　発明の数 1　（全4頁）

⑤④発明の名称　ＩＣカードシステム

㉑特　願　昭61－7882

㉒出　願　昭61(1986)1月20日

⑦②発明者　家木　俊温　横須賀市武1丁目2356番地　日本電信電話株式会社複合通信研究所内

⑦①出願人　日本電信電話株式会社　東京都千代田区内幸町1丁目1番6号

⑦④代理人　弁理士　小林　将高

明　細　書

1．発明の名称

ＩＣカードシステム

2．特許請求の範囲

ＩＣカードおよびＩＣカードの正当性のチェックを行うセンタより構成されるシステムにおいて、個々のＩＣカード毎の特有値情報の正当性を保証するためのパスワードと、通信情報の暗号化・復号化を行うための暗号・復号関数および暗号・復号鍵を更新するための鍵更新関数と、これら暗号・復号鍵、鍵更新関数の固定・可変パラメータとを、個々の前記ＩＣカードおよびセンタ内にそれぞれ格納し、かつ暗号・復号鍵の更新時に可変パラメータの変化値を前記ＩＣカードに通知する通知手段を前記センタ内に設けたことを特徴とするＩＣカードシステム。

3．発明の詳細な説明

〔産業上の利用分野〕

この発明は、ＩＣカードが、そのシステムのセンタに対して、パスワード等の情報を暗号化して送信するＩＣカードシステムに関するものである。

〔従来の技術〕

従来、ＩＣカード内のパスワード（以下ＰＷという）等の情報の暗号化に関しては、ＩＣカードリーダがカードから読み取った情報を、専用の暗号装置で暗号化してからセンタに送る方法が提案されていた。しかし、この方法の場合、犯罪者が他人のカードを不正入手してカードリーダで読むと、カード内のＩＤコード（個々のＩＣカード毎の特有値情報、以下ＩＤという）、ＰＷを知ることができる。その結果、そのＩＤ，ＰＷを格納したカードの偽造、あるいはＩＤ，ＰＷを端末のキーボードから入力しセンタに送信することによって、他人になりすまして不正取引をすることができた。

そこで、最近ではこのような問題を解決するため、カードが暗号関数を、センタが復号関数を格納し、さらに、暗号鍵の固定化を防止するため、センタからカードに対して暗号鍵を送信し、その

後、カードが暗号化を行う方式が提案されている。

第２図はこの方式の概要を示したものである。すなわち、第２図において、１０はＩＣカード、２０はセンタを示し、ＩＣカード１０内には暗号器１１を有し、センタ２０内には復号器２１と判別器２２を備えている。ＩＣカード１０が端末に装着されると、センタ２０から暗号鍵Ｋを送出する。ＩＣカード１０側ではこの暗号鍵Ｋ，ＰＷ，ＩＤを暗号器１１に入力して暗号化ＰＷつまりＥ（ＰＷ，ＩＤ，Ｋ）をセンタ２０に送り、センタ２０では復号器２１で復号してＰＷをとり出し、センタ２０内にあらかじめ記憶されているＰＷと照合を行い一致すれば取引許可の指令ＳＡをＩＣカード１０側に送り、取引を開始させる。

〔発明が解決しようとする問題点〕

しかし、この場合、ＩＤ，Ｋ，暗号化ＰＷを通信回線より盗聴されると未知数がＰＷのみであるため、暗号関数を統計的処理等により見破られる可能性がある。

この発明の目的は、暗号鍵更新関数および個々のＩＣカードに特有な更新関数の固定・可変パラメータをカード内に格納することにより、暗号鍵が犯罪者に見破られるのを防ぎ、システムのセキュリティを守ることにある。

〔問題点を解決するための手段〕

この発明にかかるＩＣカードシステムは、個々のＩＣカード毎の特有値情報の正当性を保証するためのパスワードと、通信情報の暗号化・復号化を行うための暗号・復号関数および暗号・復号鍵を更新するための鍵更新関数と、これら暗号・復号鍵、鍵更新関数の固定・可変パラメータとを個々のＩＣカードおよびセンタ内に格納し、かつ暗号・復号鍵の更新時に可変パラメータの変化値をＩＣカードに通知する通知手段をセンタ内に設けたものである。

〔作用〕

この発明は、取引の度に暗号復号鍵を更新するための可変パラメータの変化値をセンタからＩＣカードに送り、これに基づいてＩＣカードから暗

号化ＰＷをセンタに送り、センタはこれから復号関数を生成し、センタ内で照合し、一致すれば取引許可信号をＩＣカードに送る。

〔実施例〕

第１図はこの発明の一実施例の構成を示したブロック図である。この図で第２図と同じ符号は同じものを示し、１２は前記ＩＣカード１０に設けた暗号鍵更新暗号器、２３は前記センタ２０に設けた復号鍵更新暗号器、２４は通知手段で、センタ２０からＩＣカード１０へ可変パラメータの変化値を通知する。

ＩＣカード１０内には、ＩＤ，ＰＷ，暗号関数Ｅ（Ｘ）に加えて、暗号鍵更新関数Ｇ（Ｘ），Ｇ（Ｘ）の固定パラメータＡ，Ｇ（Ｘ）の可変パラメータＲ，ｉ回目の取引に用いた暗号鍵K_iが格納されている。一方、センタ２０には、ＩＣカード１０のＩＤ，ＰＷ，復号関数Ｄ（Ｘ）に加えて復号鍵更新関数Ｈ（Ｘ），Ｈ（Ｘ）の固定可変パラメータＢ，Ｒ，ｉ回目の復号鍵K_i'が格納されている。なお、固定パラメータＡ，Ｂはあらかじ

め設定しておくもので、同じ値である必要はない。

次に動作について説明する。ＩＣカード１０からセンタ２０にＩＤを送信すると、センタ２０はＩＣカード１０に可変パラメータＲの変化分△Ｒを通知手段２４から送信する。ＩＣカード１０は、暗号鍵更新関数Ｇ（Ｘ）に、K_i，Ｒ，△Ｒ，Ａを代入して新たな暗号鍵K_i+1を生成し、これに基づいた暗号化ＰＷをセンタ２０に送信する。センタ２０は、復号鍵更新関数Ｈ（Ｘ）に、K_i，Ｒ，△Ｒ，Ｂを代入して新たな復号鍵K_i+1を生成する。

その後、ＩＣカード１０は、暗号関数Ｅ（Ｘ）に、ＰＷとK_i+1を代入して暗号化ＰＷを生成し、センタ２０を送信する。センタ２０では、受信した暗号化ＰＷを復号関数Ｄ（Ｘ）を用いて復号化しＰＷをとり出し、センタ２０内のＰＷと照合し一致すれば取引許可信号ＳＡを発し、金融取引等を許可する。なお、K_i，K_i'は一致させる必要はない。

この方式では、ＩＤ，△Ｒ，暗号化ＰＷを犯罪者が盗聴しても、Ｅ（Ｘ），Ｇ（Ｘ），Ｋｉ，Ａ，Ｒが未知であるため、犯罪者がＰＷ，Ｋｉ＋１を推測するのは不可能である。したがって、犯罪者が正しい暗号化ＰＷを生成し、他人になりすまして不正取引を行うことも不可能である。

なお、第１図の場合において、暗号関数Ｅ（Ｘ）と復号関数Ｄ（Ｘ）を同じにすれば（例えば、ＰＷとＫｉ＋１の排他的論理和をとる）、Ａ＝Ｂ，Ｋｉ＝Ｋｉ，Ｇ（Ｘ）＝Ｈ（Ｘ）となり、暗号方式の簡易化がはかれる。

〔発明の効果〕

この発明においては、同一システム内で利用される全てのＩＣカードは、全ＩＣカードに共通な暗号鍵更新関数と、各ＩＣカード固有の暗号鍵、関数用固定パラメータ、可変パラメータをＩＣカードとセンタ内に格納し、取引の度に暗号復号鍵を更新するための可変パラメータの変化値を送るようにしたので、以下の利点がある。

(1) ＩＣカード内には、秘密の関数１個と、秘密のパラメータが３つあり、これらを使って情報の暗号化を行うため、暗号化情報を解読されることはない。

(2) 犯罪者が暗号鍵を知る可能性がほとんどないため、暗号関数として、ＩＣカード内のＣＰＵで実現できる簡易なものを用いることができる。

(3) 暗号関数として簡易なものを利用できるため、暗号化に要する時間が短くて良い。

(4) ＩＣカードに固有な暗号鍵、パラメータを用いるため、１つのＩＣカードについて、犯罪者が秘密情報を知り得ても、他のＩＣカードについて知ることは不可能である。

４．図面の簡単な説明

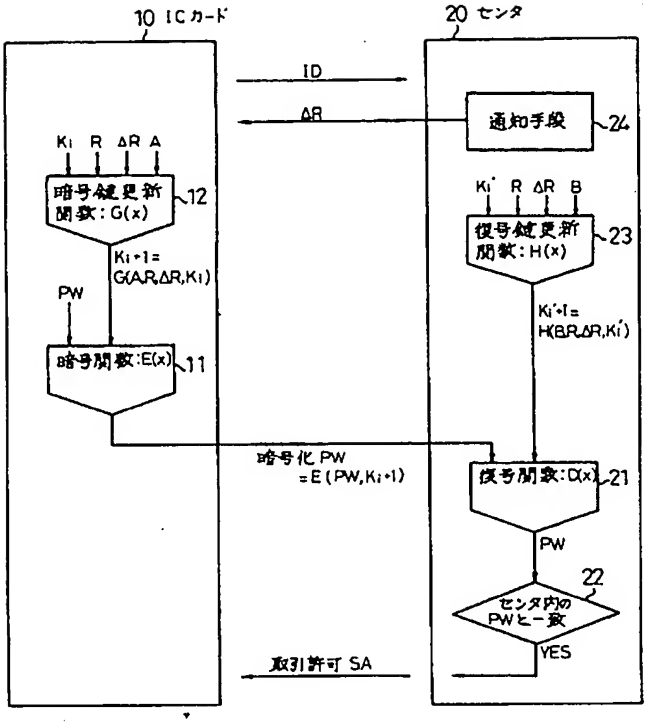
第１図はこの発明によるＩＣカード利用システムの一実施例の構成を示すブロック図、第２図は、ＩＣカード利用システム用として従来提案されていた暗号・復号方式のシステムの構成を示すブロック図である。

図中、１０はＩＣカード、１１は暗号器、１２は暗号鍵更新暗号器、２０はセンタ、２１は復号

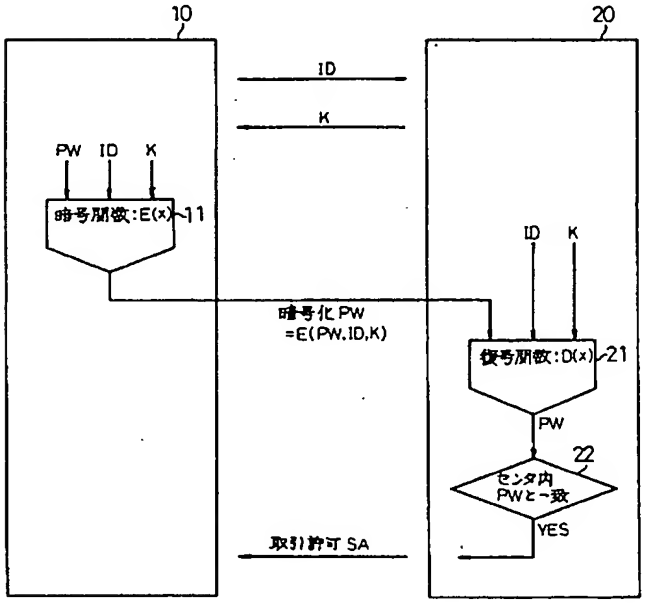
器、２２は判別器、２３は復号鍵更新暗号器、２４は通知手段である。

代理人　小　林　将　高　 

第 1 図


10 ICカード
20 センタ
ID
ΔR
通知手段
24
Ki R ΔR A
暗号鍵更新関数：G(x)
12
Ki+1=G(A,R,ΔR,Ki)
PW
暗号関数：E(x)
11
Ki' R ΔR B
復号鍵更新関数：H(x)
23
Ki'+1=H(B,R,ΔR,Ki')
暗号化 PW =E(PW,Ki+1)
復号関数：D(x)
21
PW
22
センタ内のPWと一致
YES
取引許可 SA

第 2 図


10
20
ID
K
PW ID K
暗号関数：E(x)
11
暗号化 PW =E(PW,ID,K)
ID K
復号関数：D(x)
21
PW
22
センタ内PWと一致
YES
取引許可 SA